Electronic Version
Stylesheet Version v1.1.1

Claims

[c1] 1. A method of providing a secure connection from a first end machine to a second end machine, said method being performed in said first end machine, said method comprising:

negotiating a first set of attributes of a security association (SA) with said second end machine, wherein said first set of attributes are used to provide said secure connection to said second end machine;

sending to said second end machine a first packet using said SA, wherein said first end machine is assigned a self address equaling a first address such that said first packet is sent with said first address and using said SA;

detecting that said self address is changed to a new address;

sending a request to said second end machine, wherein said new address is contained in a payload portion of a packet forming said request, said request indicating that said self address has changed to said new address; and

sending to said second end machine a second packet using said SA, wherein said second packet contains said new address as a source address,

wherein said secure connection is provided using said SA

both before and after said self_address changed such that said secure communication can be provided with minimal overhead even if said self_address changes.

[c2] 2. The method of claim 1, further comprising encrypting a portion of said payload containing said new address to generate an encrypted data and including said encrypted data in said request.

[c3] 3. The method of claim 2, further comprising including an authentication data in said payload, wherein said authentication data authenticates that said payload is sent from said first system.

[c4] 4. The method of claim 3, further comprising receiving from said second end machine a third packet in response to said second packet.

[c5] 5. The method of claim 3, wherein said second packet and said third packet relate to user applications.

[c6] 6. The method of claim 3, further comprising receiving a response from said second end machine, where said response indicates whether said new address is bound to said SA, wherein said second packet is sent after receiving said response.

[c7] 7. The method of claim 6, wherein a plurality of secure

connections are provided between said first end machine and said second end machine, wherein a plurality of SAs are present associated with corresponding ones of said plurality of secure connections, said method further comprising:

including an identifier associated with each of said plurality of SAs in said request, wherein said response indicates whether said new address is bound to all of said plurality of SAs in said second end machine.

[c8] 8. The method of claim 6, wherein said negotiating is performed according to Internet Security Association and Key Management Protocol (ISAKMP), and wherein said new address is contained in a ISAKMP portion of said payload.

[c9] 9. The method of claim 8, wherein said packet comprises an IP packet.

[c10] 10. The method of claim 6, wherein said first end device comprises a client system from which a user accesses a server system.

[c11] 11. A method of providing a secure connection from a first end machine to a second end machine, said method being performed in said second end machine, said method comprising:

negotiating a first set of attributes of a security association (SA) with said first end machine, wherein said first set of attributes are used to provide said secure connection to said first end machine;
binding said SA to a first address, wherein said first address comprises a self_address of said first end machine;
receiving a request indicating that said self_address of said first end machine is changed to a new address, wherein said new address is contained in a payload portion of a packet forming said request; and
binding said SA to said new address.

[c12] 12. The method of claim 11, wherein said payload portion is received in an encrypted format, said method further comprising decrypting said payload portion to determine said new address.

[c13] 13. The method of claim 12, further comprising:
receiving a first packet from said first end machine, wherein said first packet is received using said first address, wherein said first packet is received before receiving said request;
receiving a second packet from said first end machine, wherein said second packet is received using said new address, wherein said second packet is received after receiving said request; and
processing said first packet and said second packet us-

ing said SA.

[c14] 14. The method of claim 13, further comprising sending a response to said first end machine upon receiving said request, where said response indicates whether said new address is bound to said SA, wherein said second packet is received after sending said response.

[c15] 15. The method of claim 14, wherein a plurality of secure connections are provided between said first end machine and said second end machine, wherein a plurality of SAs are present associated with corresponding ones of said plurality of secure connections, wherein said request includes an identifier associated with each of said plurality of SAs in said request, wherein said response indicates whether said new address is bound to all of said plurality of SAs.

[c16] 16. The method of claim 13, wherein said negotiating is performed according to Internet Security Association and Key Management Protocol (ISAKMP), and wherein said request is sent consistent with a format specified by ISAKMP.

[c17] 17. The method of claim 13, wherein said first end device comprises a gateway.

[c18] 18. A computer readable medium carrying one or more

sequences of instructions for causing a first end machine to provide a secure connection to a second end machine, wherein execution of said one or more sequences of instructions by one or more processors contained in said first end machine causes said one or more processors to perform the actions of:

negotiating a first set of attributes of a security association (SA) with said second end machine, wherein said first set of attributes are used to provide said secure connection to said second end machine;

sending to said second end machine a first packet using said SA, wherein said first end machine is assigned a self address equaling a first address such that said first packet is sent with said first address and using said SA;

detecting that said self address is changed to a new address;

sending a request to said second end machine, wherein said new address is contained in a payload portion of a packet forming said request, said request indicating that said self address has changed to said new address; and

sending to said second end machine a second packet using said SA, wherein said second packet contains said new address as a source address,

wherein said secure connection is provided using said SA both before and after said self_address changed such that said secure communication can be provided with

minimal overhead even if said self_address changes.

[c19] 19. The computer readable medium of claim 18, further comprising encrypting a portion of said payload containing said new address to generate an encrypted data and including said encrypted data in said request.

[c20] 20. The computer readable medium of claim 18, further comprising including an authentication data in said packet, wherein said authentication data authenticates that said payload is sent from said first system.

[c21] 21. The computer readable medium of claim 18, further comprising receiving from said second end machine a third packet in response to said second packet.

[c22] 22. The computer readable medium of claim 21, wherein said second packet and said third packet relate to user applications.

[c23] 23. The computer readable medium of claim 18, further comprising:
sending a request to said second end machine, wherein said request indicates that said self_address has changed to said new address; and
receiving a response from said second end machine, where said response indicates whether said new address is bound to said SA, wherein said second packet is sent

after receiving said response.

[c24] 24. The computer readable medium of claim 23, wherein a plurality of secure connections are provided between said first end machine and said second end machine, wherein a plurality of SAs are present associated with corresponding ones of said plurality of secure connections, further comprising:
including an identifier associated with each of said plurality of SAs in said request, wherein said response indicates whether said new address is bound to all of said plurality of SAs in said second end machine.

[c25] 25. The computer readable medium of claim 23, wherein said negotiating is performed according to Internet Security Association and Key Management Protocol (ISAKMP), and wherein said new address is present in an ISAKMP portion of said payload.

[c26] 26. The computer readable medium of claim 23, wherein said first end device comprises a client system from which a user accesses a server system.

[c27] 27. A computer readable medium carrying one or more sequences of instructions for causing a second end machine to provide a secure connection to a first end machine, wherein execution of said one or more sequences

of instructions by one or more processors contained in said second end machine causes said one or more processors to perform the actions of:

negotiating a first set of attributes of a security association (SA) with said first end machine, wherein said first set of attributes are used to provide said secure connection to said first end machine;

binding said SA to a first address, wherein said first address comprises a self_address of said first end machine;

receiving a request indicating that said self_address of said first end machine is changed to a new address, wherein said new address is contained in a payload portion of a packet forming said request; and

binding said SA to said new address.

[c28] 28.The computer readable medium of claim 27, wherein said payload portion is received in an encrypted format, said actions further comprising decrypting said payload portion to determine said new address.

[c29] 29. The computer readable medium of claim 27, further comprising:

receiving a first packet from said first end machine, wherein said first packet is received using said first address, wherein said first packet is received before receiving said request;

receiving a second packet from said first end machine,

wherein said second packet is received using said new address, wherein said second packet is received after receiving said request; and

processing said first packet and said second packet using said SA.

[c30] 30. The computer readable medium of claim 29, further comprising:

receiving a request from said first end machine, wherein said request indicates that said self_address has changed to said new address; and

sending a response to said first end machine, where said response indicates whether said new address is bound to said SA, wherein said second packet is received after sending said response.

[c31] 31. The computer readable medium of claim 30, wherein a plurality of secure connections are provided between said first end machine and said second end machine, wherein a plurality of SAs are present associated with corresponding ones of said plurality of secure connections, wherein said request includes an identifier associated with each of said plurality of SAs in said request, wherein said response indicates whether said new address is bound to all of said plurality of SAs.

[c32] 32. The computer readable medium of claim 29, wherein

said negotiating is performed according to Internet Security Association and Key Management Protocol (ISAKMP), and wherein said new address is included in an ISAKMP portion of said payload.

[c33] 33. The computer readable medium of claim 29, wherein said first end device comprises a gateway.

[c34] 34. A first end machine providing a secure connection to a second end machine, said first end machine comprising:

means for negotiating a first set of attributes of a security association (SA) with said second end machine, wherein said first set of attributes are used to provide said secure connection to said second end machine;

means for sending to said second end machine a first packet using said SA, wherein said first end machine is assigned a self address equaling a first address such that said first packet is sent with said first address and using said SA;

means for detecting that said self address is changed to a new address;

means for sending a request to said second end machine, wherein said new address is contained in a payload portion of a packet forming said request, said request indicating that said self address has changed to said new address; and

means for sending to said second end machine a second packet using said SA, wherein said second packet contains said new address as a source address,
wherein said secure connection is provided using said SA both before and after said self_address changed such that said secure communication can be provided with minimal overhead even if said self_address changes.

[c35] 35. The first end machine of claim 34, further comprising means for encrypting a portion of said payload containing said new address to generate an encrypted data and including said encrypted data in said request.

[c36] 36. The first end machine of claim 35, further comprising means for including an authentication data in said packet, wherein said authentication data authenticates that said payload is sent from said first system.

[c37] 37. The first end machine of claim 35, further comprising receiving from said second end machine a third packet in response to said second packet.

[c38] 38. The first end machine of claim 37, wherein said second packet and said third packet are related to user applications.

[c39] 39. The first end machine of claim 34, further comprising:

means for sending a request to said second end machine, wherein said request indicates that said self_address has changed to said new address; and means for receiving a response from said second end machine, where said response indicates whether said new address is bound to said SA, wherein said second packet is sent after receiving said response.

[c40] 40. The first end machine of claim 39, wherein a plurality of secure connections are provided between said first end machine and said second end machine, wherein a plurality of SAs are present associated with corresponding ones of said plurality of secure connections, said first end machine further comprising:
means for including an identifier associated with each of said plurality of SAs in said request, wherein said response indicates whether said new address is bound to all of said plurality of SAs in said second end machine.

[c41] 41. The first end machine of claim 39, wherein said means for negotiating operates according to Internet Security Association and Key Management Protocol (ISAKMP), and wherein said new address is contained in an ISAKMP portion of said payload.

[c42] 42. The first end machine of claim 39, wherein said first end device comprises a client system from which a user

accesses a server system.

[c43] 43. A second end machine providing a secure connection to a first end machine, said second end machine comprising:
means for negotiating a first set of attributes of a security association (SA) with said first end machine, wherein said first set of attributes are used to provide said secure connection to said first end machine;
means for binding said SA to a first address, wherein said first address comprises a self_address of said first end machine;
means for receiving a request indicating that said self_address of said first end machine is changed to a new address, wherein said new address is contained in a payload portion of a packet forming said request; and
means for binding said SA to said new address.

[c44] 44. The second end machine of claim 43, wherein said payload portion is received in an encrypted format, further comprising means for decrypting said payload portion to determine said new address.

[c45] 45. The second end machine of claim 44, further comprising:
means for receiving a first packet from said first end machine, wherein said first packet is received using said

first address, wherein said first packet is received before receiving said request;

means for receiving a second packet from said first end machine, wherein said second packet is received using said new address, wherein said second packet is received after receiving said request; and

means for processing said first packet and said second packet using said SA.

[c46] 46. The second end machine of claim 45, further comprising:

means for receiving a request from said first end machine, wherein said request indicates that said self_address has changed to said new address; and

means for sending a response to said first end machine, where said response indicates whether said new address is bound to said SA, wherein said second packet is received after sending said response.

[c47] 47. The second end machine of claim 46, wherein a plurality of secure connections are provided between said first end machine and said second end machine, wherein a plurality of SAs are present associated with corresponding ones of said plurality of secure connections, wherein said request includes an identifier associated with each of said plurality of SAs in said request, wherein said response indicates whether said new address is

bound to all of said plurality of SAs.

[c48] 48. The second end machine of claim 45, wherein said negotiating is performed according to Internet Security Association and Key Management Protocol (ISAKMP), and wherein said new address is contained in an ISAKMP portion of said payload.

[c49] 49. The second end machine of claim 45, wherein said first end device comprises a gateway.

[c50] 50. A networking system comprising:
a first end device and a second end device operable to:
set up a secure connection between said first end device and said second end device, wherein said SA is bound to a first address in said second end device, wherein said first address comprises a self_address of said first end device, wherein said secure connection is based on a security association (SA);
change said self_address of said first end device to a new address;
send a request to said second end machine, wherein said new address is contained in a payload portion of a packet forming said request, said request indicating that said self address has changed to said new address; and
continue using said SA to provide said secure connection between said first end device and said second end de-

vice.

[c51] 51. The networking system of claim 50, wherein said first end system is further operable to encrypt a portion of said payload containing said new address to generate an encrypted data and include said encrypted data in said request.

[c52] 52. The networking system of claim 51, wherein said first end system is further operable to include an authentication data in said payload, wherein said authentication data authenticates that said payload is sent from said first system.

[c53] 53. The networking system of claim 52, wherein said secure connection is established according to Internet Security Association and Key Management Protocol (ISAKMP), and wherein said new address is contained in an ISAKMP portion of said payload.

[c54] 54. The network system of claim 53, wherein said first end device comprises an address block detecting that said self_address has changed from said first address to said new address, said address block sending a request to said second end device indicating that said new address is to be bound to said SA.

[c55] 55. The networking system of claim 54, wherein said

second end device comprises:

a memory storing a security association database (SAD) representing binding of SAs to corresponding self_addresses at the other end of security connections, wherein said SAD is modified to indicate that said new address is associated with said SA in response to receiving said request.

[c56] 56. The networking system of claim 55, wherein said second end device further comprises:

a connection management block negotiating a plurality of attributes with said first end device, wherein said plurality of attributes form said SA, said connection management block receiving said request and modifying said SAD to bind said SA to said new address.

[c57] 57. The networking system of claim 56, wherein said second end device comprises a gateway.

[c58] 58. A first end machine providing a secure connection to a second end machine, said first end machine comprising:

a connection management block negotiating a first set of attributes of a security association (SA) with said second end machine, wherein said first set of attributes are used to provide said secure connection to said second end machine;

an address block detecting that a self address of said first end machine is changed from a first address to a new address and sending a request to said second end machine, wherein said new address is contained in a payload of a packet forming said request, said request indicating that said self address has changed to said new address; and

a secure transmission block sending to said second end machine a first packet using said SA, wherein said first end machine is assigned a self address equaling a first address such that said first packet is sent with said first address and using said SA, said secure transmission block sending a second packet using said SA and said new address after said address block detects that said self address is changed to said new address.

[c59] 59. The first end machine of claim 58, wherein said address block encrypts a portion of said payload containing said new address to generate an encrypted data and includes said encrypted data in said request.

[c60] 60. The first end machine of claim 59, wherein said address block includes an authentication data in said payload, wherein said authentication data authenticates that said payload is sent from said first system.

[c61] 61. The first end machine of claim 60, wherein said se-

cure connection is established according to Internet Security Association and Key Management Protocol (ISAKMP), and wherein said new address is contained in an ISAKMP portion of said payload.

[c62] 62. The first end machine of claim 61, wherein said secure connection is provided using said SA both before and after said the change of said self_address such that said secure communication can be provided with minimal overhead even if said self_address changes.

[c63] 63. The first end machine of claim 62, wherein said secure transmission block receives from said second end machine a third packet in response to said second packet.

[c64] 64. The first end machine of claim 61, wherein said connection management block sends a request to said second end machine, wherein said request indicates that said self_address has changed to said new address, said connection management block receiving a response from said second end machine, where said response indicates whether said new address is bound to said SA in said second machine, wherein said second packet is sent after receiving said response.

[c65] 65. The first end machine of claim 64, wherein a plurality

of secure connections are provided between said first end machine and said second end machine, wherein a plurality of SAs are present associated with corresponding ones of said plurality of secure connections, wherein said address block includes an identifier associated with each of said plurality of SAs in said request, wherein said response indicates whether said new address is bound to all of said plurality of SAs in said second end machine.

[c66] 66. The first end machine of claim 64, wherein said connection management block operates according to Internet Security Association and Key Management Protocol (ISAKMP), and wherein said request is sent consistent with a format specified by ISAKMP.

[c67] 67. The first end machine of claim 66, wherein at least some of said first set of attributes are contained in a ISAKMP SA.

[c68] 68. A second end machine providing a secure connection to a first end machine, said second end machine comprising:
a connection management block negotiating a first set of attributes of a security association (SA) with said first end machine, wherein said first set of attributes are used to provide said secure connection to said first end machine; and

a memory storing a security association database (SAD) indicating that said SA is bound to a first address, wherein said first address comprises a self_address of said first end machine,
wherein said connection management block receives a request indicating that said self_address of said first end machine is changed to a new address, changes said SAD to indicate that said SA is bound to said new address, wherein said new address is contained in a payload portion of a packet forming said request.

[c69] 69. The second end machine of claim 68, wherein said payload portion is received in an encrypted format, said connection management block decrypting said payload portion to determine said new address.

[c70] 70. The second end machine of claim 68, further comprising a secure transmission block receiving a first packet from said first end machine, wherein said first packet is received using said first address, wherein said first packet is received before receiving said request, said secure transmission block receiving a second packet from said first end machine, wherein said second packet is received using said new address, wherein said second packet is received after receiving said request,
wherein said secure transmission block processes said first packet and said second packet using said SA.

[c71] 71. The second end machine of claim 70, wherein said connection management block receives a request from said first end machine, wherein said request indicates that said self_address has changed to said new address, said connection management block sending a response to said first end machine after changing said SAD, wherein said response indicates whether said new address is bound to said SA, wherein said second packet is received after sending said response.

[c72] 72. The second end machine of claim 71, wherein a plurality of secure connections are provided between said first end machine and said second end machine, wherein a plurality of SAs are present associated with corresponding ones of said plurality of secure connections, wherein said request includes an identifier associated with each of said plurality of SAs in said request, wherein said response indicates whether said new address is bound to all of said plurality of SAs.

[c73] 73. The second end machine of claim 70, wherein said negotiating is performed according to Internet Security Association and Key Management Protocol (ISAKMP), and wherein said request is sent consistent with a format specified by ISAKMP.

[c74] 74. The first end machine of claim 73, wherein at least some of said first set of attributes are contained in a ISAKMP SA.

[c75] 75. The second end machine of claim 70, wherein said first end device comprises a gateway.